

TUGAS AKHIR

PERANCANGAN SISTEM KEAMANAN WEB MENGUNAKAN METODE RANDOM FOREST (STUDI KASUS : INSTITUSI X)



Disusun Oleh :

MUHAMMAD FIRMAN PRAYOGI

21.18.031

**PROGRAM STUDI TEKNIK INFORMATIKA S-1
FAKULTAS TEKNOLOGI INDUSTRI
INSTITUT TEKNOLOGI NASIONAL MALANG
2025**

LEMBAR PERSETUJUAN DAN PENGESAHAN
PERANCANGAN SISTEM KEAMANAN WEB
MENGUNAKAN METODE RANDOM FOREST
(STUDI KASUS: INSTITUSI X)

TUGAS AKHIR

*Disusun dan Diajukan Sebagai Salah Satu Syarat Untuk Memperoleh Gelar
Sarjana Komputer Strata Satu (S-1)*

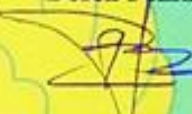


Disusun Oleh:
Muhammad Firman Prayogi
21.18.031

Diperiksa dan Disetujui,

Dosen Pembimbing I

Dr. Ahmad Fahrudi Setiawan, S.Kom., M.T.
NIP.P. 1031500497

Dosen Pembimbing II

F.X. Ariwibisono, S.T., M.Kom.
NIP.P. 1030300397

Mengetahui,
Ketua Program Studi Teknik Informatika S-1

Yosep Agus Pranoto, S.T., M.T.
NIP.P. 1031000432

PROGRAM STUDI TEKNIK INFORMATIKA S-1
FAKULTAS TEKNOLOGI INDUSTRI
INSTITUT TEKNOLOGI NASIONAL MALANG

2025

LEMBAR KEASLIAN

PERNYATAAN KEASLIAN TUGAS AKHIR

Sebagai mahasiswa Program Studi Teknik Informatika S-1 Fakultas Teknologi Industri Institut Teknologi Nasional Malang, yang bertanda tangan di bawah ini, saya:

Nama : Muhammad Firman Prayogi

NIM : 2118031

Program Studi : Teknik Informatika S-1

Fakultas : Fakultas Teknologi Industri

Menyatakan dengan sesungguhnya bahwa tugas akhir saya dengan judul **"Perancangan Sistem Keamanan Web Menggunakan Metode Random Forest (Studi Kasus : Institusi X)"** merupakan karya asli dan bukan merupakan duplikat dan mengutip seluruhnya karya orang lain. Apabila di kemudian hari, karya asli saya di sinyalir bukan merupakan karya asli saya, maka saya akan bersedia menerima segala konsekuensi apapun yang di berikan Program Studi Teknik Informatika S-1 Institut Teknologi Nasional Malang.

Demikian surat pernyataan ini saya buat dengan sebenar-benarnya.

Malang, 14 Juli 2025



(Muhammad Firman Prayogi)

NIM. 2118031

PERANCANGAN SISTEM KEAMANAN WEB MENGGUNAKAN METODE RANDOM FOREST (STUDI KASUS : INSTITUSI X)

Muhammad Firman Prayogi, Ahmad Fahrudi Setiawan, Franciscus

Xaverius Ariwibisono

Teknik Informatika, Institut Teknologi Nasional Malang

Jalan Raya Karanglo km 2 Malang, Indonesia

muhammadfirmanprayogi@gmail.com

ABSTRAK

Penelitian ini bertujuan mengembangkan *SecureShield* Web Security Defender, sebuah sistem keamanan web berbasis *machine learning* untuk mendeteksi serangan *SQL Injection*, *Webshell*, dan *Cross site scripting (XSS)*. Sistem ini menggunakan algoritma Random Forest sebagai model klasifikasi, dengan arsitektur modular yang terdiri dari Go Agent sebagai pemantau lalu lintas, Python Engine sebagai pemroses data, dan Dashboard sebagai antarmuka pengguna. Data dilatih dan dievaluasi menggunakan metrik akurasi, presisi, recall, dan F1-Score. Hasil menunjukkan bahwa sistem mencapai akurasi deteksi lebih dari 93% pada ketiga jenis serangan. Sistem juga mampu merespons secara *real-time* dengan latency rata-rata 1.3 detik. Sistem ini memberikan kontribusi dalam mendeteksi ancaman siber secara otomatis, adaptif, dan terintegrasi dalam satu platform monitoring.

Kata kunci : *Web security, XSS ,SQL Injection, Webshell, Random forest, Real-time monitoring*

KATA PENGANTAR

Segala puji dan syukur penulis panjatkan ke hadirat Tuhan Yang Maha Esa, karena atas limpahan rahmat, kasih sayang, dan kekuatan dari-Nya, penulis dapat menyelesaikan skripsi yang berjudul: **“Perancangan Sistem Keamanan Web Menggunakan Metode Random Forest (Studi Kasus: Institusi X)”** Skripsi ini disusun sebagai salah satu syarat untuk memperoleh gelar Sarjana pada Program Studi Teknik Informatika, Fakultas Teknologi Industri, Institut Teknologi Nasional Malang. Penyusunan skripsi ini bukanlah perjalanan yang mudah. Di balik setiap proses yang dilalui, penulis merasakan betapa besar arti dukungan dan doa dari keluarga tercinta. Ucapan terima kasih yang mendalam penulis sampaikan kepada ayah Sudaramanto dan terutama kepada almarhumah ibu Hindun Habibu, yang meskipun telah berpulang ke sisinya pada tanggal 4 Desember 2024, cinta dan pengorbanannya tetap menjadi cahaya penuntun dalam setiap langkah. Dengan ini penulis juga mengucapkan terima kasih dan penghargaan yang sebesar-besarnya kepada:

1. Allah SWT atas segala nikmat dan kemudahan yang telah diberikan selama proses ini.
2. Bapak Yosep Agus Pranoto, ST., MT., selaku Ketua Program Studi Teknik Informatika S-1 ITN Malang.
3. Dr. Ahmad Fahrudi Setiawan, S.Kom., M.T., selaku Dosen Pembimbing Utama yang telah memberikan arahan, ilmu, dan motivasi yang berarti.
4. F.X. Ariwibisono, S.T., M.Kom., selaku Dosen Pembimbing Pendamping atas bimbingan dan evaluasi yang membangun.
5. Saudara dan saudari tersayang Rengga Eka Sarvian Mangun Redjo, Dwi Juanda Mangun Redjo, Triana Fadila Gerhana Putri, dan Artika Yunisma Putri yang dengan caranya masing-masing telah menjadi sumber kekuatan.
6. Sahabat dan rekan seperjuangan yang telah menjadi tempat berbagi semangat, tawa, dan perjuangan selama masa studi.

Akhir kata, penulis berharap skripsi ini dapat memberikan manfaat bagi semua pihak yang membacanya, serta menjadi kontribusi kecil dalam pengembangan ilmu di bidang keamanan sistem informasi.

Malang, 14 Juli 2025

Penulis

DAFTAR ISI

ABSTRAK	iv
KATA PENGANTAR	v
DAFTAR ISI.....	vi
DAFTAR GAMBAR	viii
DAFTAR TABLE.....	x
BAB I	11
LATAR BELAKANG	11
1.1 Latar Belakang	11
1.2 Rumusan Masalah	13
1.3 Tujuan.....	13
1.4 Batasan Masalah.....	13
1.5 Manfaat.....	13
1.6 Metode penelitian	14
1.7 Sistematika Penilaian	15
BAB II.....	16
TINJAUAN PUSTAKA	16
2.1 Penelitian Terdahulu.....	16
2.2 Konsep Dasar Serangan.....	18
2.3 Jenis-Jenis Serangan.....	20
2.4 <i>Random Forest</i>	23
2.5 <i>TF-IDF</i>	23
BAB III	25
ANALISIS PERANCANGAN	25
3.1 Arsitektur Sistem.....	25
3.2 Kebutuhan Fungsional.....	25

3.3	Kebutuhan non fungsional.....	26
3.4	Prioritas kebutuhan dan analisis serangan.....	27
3.5	Use case diagram.....	28
3.6	Struktur menu	29
3.7	Flowchart Dan Diagram Blok Sistem	30
3.8	Skenario pengujian	38
3.9	Prototype Desain	40
BAB IV		41
IMPLEMENTASI DAN PENGUJIAN		41
4.1	Implementasi	41
4.2	Lingkungan Pengujian.....	41
4.3	Evaluasi Kinerja Model <i>Machine Learning</i>	41
4.4	Implementasi Komponen Sistem <i>SecureShield</i>	48
4.5	Pengujian Fungsional dan Skenario Serangan <i>End-to-End SecureShield</i> 53	
4.6	Pengujian Ketahanan Sistem (<i>Stress Test</i>)	58
BAB V.....		61
PENUTUP.....		61
5.1	Kesimpulan.....	61
5.2	Saran	62
DAFTAR PUSTAKA		64
LAMPIRAN.....		67

DAFTAR GAMBAR

Gambar 2.1 <i>SQL Injection</i> (source: https://www.arkoselabs.com/wp-content/uploads/Malicious-SQL-Injection-Attack.png).....	18
Gambar 2.2 Tampilan sebelum di deface(source: https://www.unila.ac.id/dwp-gelar-workshop-evaluasi-dan-penyusunan-progja-2025-di-kali-bronjong-pesawaran/)	19
Gambar 2.3 Tampilan setelah di <i>deface</i> (source: https://dwp.unila.ac.id)	19
Gambar 2.4 Skema <i>Web Defacement</i> (Id-SIRTII /CC, 2023).....	22
Gambar 3.1 Use case diagram <i>secureshield</i>	28
Gambar 3.2 Struktur menu dashboard	29
Gambar 3.3 Flowchart Agent reverse proxy	30
Gambar 3.4 Flowchart Engine	32
Gambar 3.5 Penggunaan <i>randomforest</i> untuk XSS	33
Gambar 3.6 Penggunaan <i>randomforest</i> untuk <i>SQLi</i>	34
Gambar 3.7 Penggunaan <i>randomforest</i> untuk <i>Webshell</i>	35
Gambar 3.8 Flowchart sistem	37
Gambar 3.9 Skenario pengujian.....	38
Gambar 3.10 Log serangan	40
Gambar 4.1 GridSearch deteksi <i>SQL Injection</i>	42
Gambar 4.2 Confusion matrix <i>SQL Injection</i>	42
Gambar 4.3 Confusion matrix XSS	43
Gambar 4.4 GridSearchCV <i>Webshell</i>	44
Gambar 4.5 Confusion Matrix <i>Webshell</i>	44
Gambar 4.6 Tampilan <i>dashboard</i>	48
Gambar 4.7 Tampilan <i>Alerts</i>	48
Gambar 4.8 Tampilan Reports	49
Gambar 4.9 Tampilan <i>settings</i>	49

Gambar 4.10 <i>Agent</i> sebelum monitoring	51
Gambar 4.11 <i>Agent active monitoring</i>	51
Gambar 4.12 <i>Python engine</i>	52
Gambar 4.13 Uji kesehatan layanan <i>Engine</i>	53
Gambar 4.14 <i>Agent</i> dan <i>monitoring activated</i>	53
Gambar 4.15 Uji kesehatan layanan <i>Agent</i>	54
Gambar 4.16 <i>Inject</i> serangan <i>target</i> belum menggunakan <i>securshield</i>	54
Gambar 4.17 <i>Inject</i> pada <i>target</i> yang telah menggunakan <i>securshield</i>	55
Gambar 4.18 <i>Inject</i> serangan <i>target</i> belum menggunakan <i>securshield</i>	55
Gambar 4.19 <i>Inject</i> pada <i>target</i> yang telah menggunakan <i>securshield</i>	56
Gambar 4.20 <i>inject</i> serangan <i>target</i> belum menggunakan <i>securshield</i>	56
Gambar 4.21 <i>Inject</i> pada <i>target</i> yang telah menggunakan <i>securshield</i>	57
Gambar 4.22 Hasil Uji ketahanan sistem dengan skrip stress test.py	58

DAFTAR TABLE

Tabel 2.1 sintaks <i>SQL Injection</i> yang biasa digunakan oleh peretas untuk membobol situs <i>web</i> (Ferdianto, Yovie, 2023)	20
Tabel 3.1 Kebutuhan fungsional	25
Tabel 3.2 Kebutuhan non-fungsional	26
Tabel 3.3 Prioritas kebutuhan	27
Tabel 3.4 Analisis Kebutuhan dengan Ancaman Siber.....	27
Tabel 4.1 Performa Model Pada Data Uji Statis	45
Tabel 4.2 Performa Model Pada Data Uji yang belum dikenal(<i>Zero-day</i>)	46
Tabel 4.3 Hasil pengujian <i>end-to-end</i>	58
Tabel 4.4 Hasil uji ketahanan sistem.....	59
Tabel 4.5 Hasil Pengujian Blackbox lengkap Setiap Komponen Sistem <i>SecureShield</i>	59